UNITED STATES DISTRICT COURT
DISTRICT OF VERMONT

UNITED STATES OF AMERICA	)	
	)	
v.	)	Docket No. 2:21-cr-66-1-cr
	)	
SCOTT REMICK,	)	
Defendant.	)	

GOVERNMENT'S OPPOSITION TO MOTION TO SUPPRESS EVIDENCE AND REQUEST FOR A *FRANKS HEARING*

The United States of America, by and through its attorney, Nikolas P. Kerest, United States Attorney for the District of Vermont, hereby files its opposition to defendant Scott Remick's Motion to Suppress Evidence and Request for a *Franks* hearing (the Motion). (Doc. 71). For all of the reasons that follow, the Motion should be denied.

I. INTRODUCTION

On June 16, 2021, a private computer security analyst (the SOI) accessed digital media on Scott Remick's network through a vulnerability the SOI was researching. While in Remick's media, the SOI saw child sexual abuse material (CSAM, or child pornography) and content that led him[1] to believe that Remick was sexually exploiting a minor. The SOI took some content (no CSAM) to identify Remick and his location, created a "backdoor" so he could get into Remick's media again if the vulnerability was cured, and notified law enforcement, even though in doing so the SOI implicated himself in a crime.

Upon learning of the SOI's actions and after instructing him not to reenter Remick's media or modify anything he had already done while in the media, agents with Homeland Security Investigations (HSI) set about evaluating the SOI's information and getting warrants to

[1] The government refers to the SOI using the male pronoun in this public filing to protect the SOI's identity.

search Remick's digital media both remotely and at his residence. On July 2, 2021, Magistrate Judge Doyle issued the warrants. The next day, an alarm the SOI set up while in Remick's media went off, indicating that Remick had opened an encrypted drive. The government executed the remote warrant that day using code it wrote based on code the SOI provided. The government executed the residence warrant three days later.

Remick seeks suppression of evidence obtained through these warrants, making a variety of claims including that the SOI was a government agent, that the warrants were not supported by probable cause and were overbroad, and that the government withheld material information from the issuing court such that a *Franks* hearing should occur. For the reasons that follow, Remick's motion should be denied. In any event, the government relied in good faith on the issuance of the search warrants, and suppression should be denied on this basis as well.

II. PROCEDURAL HISTORY

On July 2, 2021, the government obtained two search warrants: one to access digital media using Remick's IP address provided by his Internet Service Provider (ISP) to connect to the Internet (the Remote Access Warrant) (Doc. 5), and one to search Remick's residence located at 1153 Hardscrabble Road in Bristol, Vermont (the Hardscrabble Road Warrant) (Doc. 1) (collectively, the Warrants). The Warrants sought evidence of violations of 18 U.S.C. §§ 2252(a)(1), (a)(2), and (a)(4).

On July 3, 2021, the government executed the Remote Access Warrant. The government exfiltrated (extracted) CSAM and other content from Remick's media. (Doc. 11-1).

On July 7, 2021, the government executed the Hardscrabble Road Warrant. During a search of media seized pursuant to this warrant, law enforcement found additional CSAM. Remick was arrested and charged by complaint that day. (Doc. 11, 11-1).

On July 22, 2021, the grand jury returned a single-count indictment against Remick which charged him with violating 18 U.S.C. §2252(a)(4)(B), possession of CSAM. (Doc. 25).

On December 10, 2021, the government obtained a warrant to search an email account (the MEGC account). This warrant sought evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A, and 2422(b). (Doc. 34).

On April 27, 2022, the government obtained a second warrant to search the devices seized pursuant to the Hardscrabble Road Warrant. This warrant authorized the search of the devices for evidence of the following additional violations: 18 U.S.C. §§ 2251, 2422(b). (Doc. 53).

On June 2, 2022, the grand jury returned a First Superseding Indictment. (Doc. 57). The nine-count superseding indictment charged Remick with the following additional charges: receipt, distribution, and production of CSAM, in violation of 18 U.S.C. §§ 2251, 2252, and with using a facility of interstate/foreign commerce to entice a minor to engage in conduct for which a person could be held criminally liable, in violation of 18 U.S.C. § 2422(b).

III. THE SEARCH WARRANTS

The Remote Access Warrant and the Hardscrabble Road Warrant relied on the same statement of probable cause, which is set forth below:

On June 16, 2021, a source of information (SOI) contacted the Vermont State Police (VSP) by phone to report that an individual living in Bristol, Vermont, later identified as Remick, was in possession of CSAM. (Doc. 5-3 at ¶ 7).[2] The SOI also sent an email to VSP where he disclosed the following, among other things:

- The SOI identified himself as a security researcher who wrote a program that scans the Internet for misconfigured computers. The program runs a bot which accessed Remick's

[2] Paragraph references relate to the Remote Access Warrant, Doc. 5.

computer through an unsecured hole in Remick's network. Through this hole, the bot was able to view "a great deal of child porn."

- The SOI was "not sure how to handle this and I am attempting to do the moral thing here."
- The SOI provided a copy of Remick's Vermont driver's license, Remick's IP address, and a text file that listed files he saw in one part of Remick's encrypted drive.
- The SOI "only had the stomach to open 7 images and they were all child porn."
- The SOI was concerned that Remick's computer network contains "TB's [terabytes] of content on various encrypted devices." The SOI shared that "you will need some cooperation with him to gain full access to all these files if they are indeed secured correctly" because "unplugging or detaching" the encrypted devices would result in "the drives locking and all the content becoming unavailable."
- The SOI added that Remick is "running a variety of services on TOR which I assume he is using to receive and transmit this data. From my perspective, I can only imagine what these devices are for and I frankly don't want to know."
- The SOI concluded the email with "This is the evidence I have. I apologize if this is not enough, I again am just attempting to do the right thing here. What I saw shook me to my core and I honestly could have never imagined being here in this position. This is fairly routine and innocuous research I do with a private team that analyzes the impact of security breaches."

(Doc. 5-3 at ¶ 7).

The affiant, HSI Special Agent (SA) Michael McCullagh, reviewed the text file provided by the SOI. SA McCullagh noted that the file did not contain content, just file titles. The file titles included "(XXXX) German Girl 14 Years Masturbation on Webcam.avi," "10Yo Girl Spreads And Plays With Hairless Pussy For Webcam – 2004.avi," "Julia 7yo – First Assfuck.avi.avi," and "10Yo Nadian REALLY CUMS!!! Masturbates Very Pink Pussy On Webcam!.avi." The agent added that he found many filenames on the SOI's text file that contained terms commonly used to identify child exploitation material. (Doc. 5-3 at ¶ 8).

The following day, on June 17, 2021, SA McCullagh and HSI SA Alex Zuchman spoke with the SOI, who disclosed the following, among other things:

- The SOI is a private software developer and security analyst. He is part of a group of individuals who analyze a specific piece of software with a specific security vulnerability. They use a "bot" to search for this vulnerability. [SA McCullagh defined a "bot" as a software program that performs automated, repetitive pre-defined tasks.]

- The SOI observed that the computer (Target Media) was using a Linux Operating System and LUKS. [SA McCullagh added that LUKS is full disk encryption for the Linux Operating System.]

- The Target Media had a mounted VeraCrypt volume (called VeraCrypt 1). The SOI saw two other folders labeled VeraCrypt 2 and VeraCrypt 3. [SA McCullagh explained that a VeraCrypt volume is "a container that has a potentially unbreakable level of encryption." The agent added that being "mounted" means that "the files/directories on storage media is available for users to access through the file system."]

- The SOI saw the presence of a TOR (the Onion Router) browser on the Target Media. [SA McCullagh added that through his training and experience, he knew that while the TOR browser has many uses, both legal and illegal, "it is commonly used by persons who are interested in child pornography because the user's identity is, generally, obscured."]

- The SOI looked at five or six, maybe seven, image files in VeraCrypt 1. The SOI identified these files as depicting child pornography. The SOI thought that there were "many additional images in the VeraCrypt 1 volume."

- The SOI viewed email messages and recalled seeing a folder named "to jenny," or something like that. In this folder, the SOI saw what he believed were additional images of child pornography. [SA McCullagh added that he looked on the text file from the SOI for a folder that included the names "Jenny" or "Jennie," but he did not find any. The agent found many files with the name "Jenny" in the filename, and two directories with the name "Jeanie" in the name: "For Jeanie/Pearl Lolitas" and "For Jeannie/Videos." SA McCullagh added that based on his training and experience, he knows that the term "Lolita" can refer to child pornography.]

(Doc. 5-3 at ¶ 9).

The following information about the SOI was set forth:

- The SOI has mental health issues that require him to take medication. The medication does not affect the SOI's faculties or recall; it is to address mood and depression issues.

- The SOI has no criminal history.

- The SOI initially spoke with the government voluntarily and without any agreement. Beginning on June 23, 2021, the SOI's disclosures were made pursuant to a "proffer letter" agreement. On June 28, 2021, the government and the SOI entered into a letter

> immunity agreement, which granted the SOI immunity co-extensive with 18 U.S.C. § 6001, *et seq.,* for disclosures he made pursuant to the agreement.

(Doc. 5-3 at n.2).

On June 30, 2021, the SOI met again with law enforcement and disclosed the following, among other information:

- When the SOI initially accessed the computer (Computer 1, part of the Target Media) associated with Remick, the IP address resolved to Germany. Because of the network configuration of Computer 1, the SOI suspected that the computer was not physically located in Germany, despite the IP address. The SOI queried another computer (Computer 2) on the same local network as Computer 1 to report its public IP address. Computer 2 responded with an IP address that resolved to an Internet Service Provider (ISP) located in Vermont (the Vermont IP address).

- The SOI deduced that Computer 1 was using a Virtual Private Network (VPN) to make it appear to be elsewhere and to conceal its true location. Computer 2 was not using a VPN so when the SOI queried it for its IP address, Computer 2 responded with the true IP address and the actual physical location of the devices.

- The SOI believed that the Vermont IP address was the true IP address because the user of Computer 1 was "Scott," the SOI found a Vermont driver's license for Scott I. Remick of Bristol, Vermont saved on the Target Media, and the IP address resolved to a Vermont ISP.

(Doc. 5-3 at ¶ 10).

SA McCullagh researched the Vermont IP address and learned that it was assigned to Waitsfield and Champlain Valley Telecom. A subpoena issued to Waitsfield and Champlain Valley Telecom revealed that the subscriber to the Vermont IP address at the date and time the SOI accessed the Target Media was Scott Remick at 1153 Hardscrabble Road, Bristol, Vermont. (Doc. 5-3 at ¶ 11). SA McCullagh also determined by researching Vermont Department of Motor Vehicles (DMV) databases that the Vermont driver's license provided by the SOI was assigned to Scott I. Remick at the Hardscrabble Road address. (Doc. 5-3 at ¶ 12).

SA McCullagh conducted open-source research into Remick and learned that Remick worked for Middlebury College as a Senior Technology Specialist. Remick also had a computer

business called "vtgeek.com." On his vtgeek.com website, in addition to setting forth his various certifications and computer expertise, Remick described himself as having "an unmatched skill set [and] decades of experience." (Doc. 5-3 at ¶ 13). Remick's website provided a phone number that was the same number in the response provided by Waitsfield and Champlain Valley Telecom. (Doc. 5-3 at ¶¶ 13, 14).

Law enforcement conducted surveillance of the Hardscrabble Road residence and observed a vehicle in the driveway that matched the vehicle Remick registered with the Vermont DMV. (Doc. 5-3 at ¶ 15).

On June 22, 2021, SA McCullagh received a CyberTip from the National Center for Missing and Exploited Children (NCMEC) from Commander Matt Raymond at the Vermont Internet Crimes Against Children Task Force (the ICAC). This CyberTip related to a call the SOI made to NCMEC on June 16, 2021 at approximately 9:01 pm, approximately one hour after he accessed Remick's computer. (Doc. 5-3 at ¶ 16).

NCMEC reported that the SOI disclosed the following in the call, among other details:

- Remick's name, date of birth, physical address, IP address, Facebook page, and employment.
- Remick had a large amount of child pornography on an encrypted drive, which was unencypted when the SOI accessed it.
- Remick is exchanging child pornography with another on the Tor network. Remick may be in a sexual relationship with that person, named Jeanie, who may be a teenager. An email address for Jeanie was provided.
- Remick will attempt to delete the child pornography if confronted by law enforcement.
- The SOI was advised to contact law enforcement if he believed his information was time-sensitive.

(Doc. 5-3 at ¶ 17).

On June 23, 2021, the agents met with the SOI, who provided descriptions of the images he saw on Remick's computer. The SOI did not save any of the images he viewed and provided the following descriptions from memory:

- A female child, approximately 10-14 years old, engaged in a sex act with a much older adult male. The SOI described the sex act as "69." [SA McCullagh included that he understood "69" to mean both individuals performing oral sex on the other.]
- A female child, approximately 12-13 years old, fully nude with her legs spread wide open. The SOI did not see any pubic hair or breast development on the child.
- A European teen, possibly Scandinavian, who was approximately 15-16 years old. She was topless and her breasts were exposed.

(Doc. 5-3 at ¶ 18).

The affidavit also disclosed that the SOI installed two separate methods to access the Target Media at a later time in case the vulnerability that allowed him access no longer existed. The SOI called these methods a "backdoor" and installed it so law enforcement would be able to access the Target Media. The SOI also installed what was called the "Ping" in the affidavit. The Ping was installed to keep the backdoor open and viable. The Ping did not access content from, or communicate with, the Target Media. Its function was to keep the communication line to the backdoor open. [SA McCullagh added that based on his training and experience, he knew a backdoor to be a "typically covert method of bypassing normal authentication or encryption in a computer, as well as other devices. Backdoors are most often used for securing remote access to a computer, allowing access to privileged information such as passwords or data on hard drives."] (Doc. 5-3 at ¶ 19).

The affidavit described typical characteristics of CSAM collectors. (Doc. 5-3 at ¶ 22).

The affidavit disclosed how the Remote Access Warrant would be executed. First, SA McCullagh explained the rationale for seeking the Remote Access Warrant: to conceal his

activities, Remick used encryption on the Target Media, which encryption would be triggered if the Target Media was unplugged or detached. If that happened, "all the content [would become] unavailable." The affidavit disclosed that the remote search of the Target Media "will entail law enforcement remotely communicating with the Target Media in order to conduct an exfiltration of the information outlined in Attachment B to a government-controlled infrastruture, meaning government-controlled storage media. Law enforcement will not make any changes to the Target Media beyond any changes to metadata that will occur as a result of accessing data during the search." (Doc. 5-3 at ¶¶ 23-24).

IV. EXECUTION OF THE REMOTE SEARCH WARRANT

A. The HSI Code

The SOI provided the details of how he infiltrated Remick's devices and the code he used (the SOI Code) to HSI Cyber Operations Officer (COO) Elijah Brigham. Brigham then used the SOI Code as a blueprint from which he wrote the code law enforcement would use (the HSI Code) during execution of the Remote Search Warrant. Brigham created the HSI Code to ensure that neither the SOI nor his computer had any involvement with execution of the warrant, to ensure that the code used for the exfiltration did only what law enforcement wanted it to do, and to ensure that the exfiltration download went to a secure receptacle controlled by the government. Once Brigham wrote the HSI Code, he recreated on a government computer what he understood the configurations of Remick's media to be, including the vulnerability exploited by the SOI. Brigham then tested the HSI Code and confirmed that it would work to exfiltrate content from Remick's digital media. When Brigham conducted the exfitration of Remick's media, he used the HSI Code, not the SOI Code. He did not use the backdoor set up by the SOI.

Also, while the SOI was consulted during the exfiltration, he was not present or otherwise involved in it.

B. The Operational Plan for Execution of the Remote Search Warrant

The government obtained the Warrants on Friday, July 2, 2021. The government planned to execute the Remote Access Warrant on Tuesday, July 6, 2021, after the Fourth of July federal holiday. At approximately 10:29 am on Saturday, July 3, 2021, the SOI reached out to the agents and sent a text message that read: "Good morning, I know its Saturday but my backdoor alarm just tripped. The Veracrypt was mounted. Is there any chance you can move today?" SA McCullagh responded that law enforcement was not in a position to execute the warrant that day. Ultimately, the agents executed the Remote Search Warrant that day.

V. LEGAL FRAMEWORK AND ANALYSIS

A. The Alarm Resulted from the Actions of a Private Actor Without Any Government Involvement

1. Statement of the Law

It is well-established that the Fourth Amendment only applies to government action. It is "wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any government official." *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). *See United States v. Steiger,* 318 F.3d 1039 (11th Cir. 2003) (anonymous computer user who hacked without government's knowledge into defendant's computer and discovered CSAM conducted private search); *United States v. Jarrett*, 338 F.3d 339 (4th Cir. 2003) (same). A search

> conducted by private individuals at the instigation of a government officer or authority may sometimes be attributable to the government for purposes of the Fourth Amendment; but private actions are generally attributable to the government only where there is a sufficiently close nexus between the State and

> the challenged action of the … entity so that the action of the latter may be fairly treated as that of the State itself. The requisite nexus is not shown merely by government approval or of acquiescence in the activity[.] The purpose of the close-nexus requirement is to assure that constitutional standards are invoked only when it can be said that the government is *responsible* for the specific conduct of what the accused complains.

United States v. DiTomasso, 932 F.3d 58, 67 (2d Cir. 2019) (internal quotation marks and citations omitted) (monitoring of user account by social networking site and submission of information to NCMEC as required by law not government action) (emphasis in original).

Whether a private actor "should be deemed an agent or instrument of the Government for Fourth Amendment purposes necessarily turns on the degree of the Government's participation in the private party's activities, a question that can only be resolved in light of the circumstances." *United States v. Guillette,* 2021 WL 1589290, *4 (D. Vt. Apr. 23, 2021) (quoting *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602, 614 (1989)). The party objecting to the search has the burden of establishing by a preponderance of the evidence that the government involvement "was significant enough to change the character of the search." *Id.* at *4 (citing *United States v. Couch*, 378 F. Supp. 2d 50, 55 (N.D.N.Y. 2005) (citing *United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987))). In deciding whether a private person acted as a government agent, courts consider: "(i) whether the government knew of and acquiesced in the citizen's conduct, (ii) whether the citizen intended to assist law enforcement, and (iii) whether the citizen acted at the government's request." *United States v. Stephen*, 984 F.3d 625, 629 (8th Cir. 2021).

If the government was involved in a search before the object of the search was completely accomplished, the government may be deemed to have participated in it. It is "immaterial whether the government originated the idea for a search or joined it while it was in progress." *United States v. Knoll,* 16 F.3d 1313, 1320 (2d Cir. 1994) (citing to *Lustig v. United*

States, 338 U.S. 74, 78-79 (1949)). The government may become a party to a search through "nothing more than tacit approval." *Id.*

The facts of *Knoll* are worth examining. Hoping to receive beneficial treatment from the government, a federal inmate orchestrated the burglary of Knoll's law office to obtain incriminating information about Knoll. The stolen materials were given to an Assistant United States Attorney (AUSA). After reviewing the materials, the AUSA expressed disappointment and told the inmate he would have to "get me more information," and "you've got to turn more over. If there's stuff out there, you've got to turn it over." *Id.* at 1320. Thereafter, the inmate caused the delivery of another batch of stolen material. After further review by the AUSA, incriminating items were found and Knoll's prosecution ensued. *Id.* at 1317. In remanding for further fact-finding, the court of appeals distinguished between the initial delivery and review of stolen materials to the government, and the delivery of additional materials after the AUSA asked for more. With the AUSA's request, the character of the search changed because it was not clear whether all of the materials from Knoll's office had already been opened, and thus Knoll's expectation of privacy already defeated by the private search. The court remanded to determine whether the private search of the stolen materials had already been completed, or if the AUSA's direction to "get me more information" was tacit approval for a further private search, thus implicating the Fourth Amendment. *Id.* at 1319-20.

2. Argument

The SOI accessed Remick's media, took content, and left in place the backdoor (for access in case the original vulnerability was cured), the Ping (to communicate with the backdoor to keep it viable), and the Alarm (to alert when Remick mounted the encrypted VeraCrypt container) on June 16, 2021. It is undisputed that the SOI took these actions without the

government's knowledge. When the SOI first spoke with law enforcement, he was instructed not to go back into Remick's media. That admonition was repeated on several occasions. There is no evidence to suggest, much less establish, that the SOI disregarded that instruction.[3] Remick cannot meet his burden of showing by a preponderance of the evidence that the government was involved in the SOI's actions, or that the government's involvement after the SOI disclosed what he had done changed the character in any way of what the SOI had already set up.

Remick complains that the Alarm constituted a warrantless search that should be attributed to the government. This complaint is without merit for the following reasons:

- First, as previously noted, everything the SOI did with Remick's media was set up without the government's knowledge. The government is simply not responsible for actions taken by the private actor during its intrusion into Remick's media and about which the government had no notice or involvement.

- Second, instructing the SOI to return to Remick's media to remove the Alarm would have resulted in a warrantless entry done at the government's direction – an illegal search. Rather than to secure process to remove that which it had not authorized or installed, the government worked as quickly as possible to obtain a search warrant. Indeed, there are no apparent means by which a court could have authorized a return to Remick's media to disable the Alarm as Fed. R. Crim. P. 41 would not have allowed that action. Further, to the extent it is suggested that the SOI could have simply shut down his computer and terminated that which he set up, exigent circumstances justified keep what he set in place intact. If the vulnerability exploited by the SOI was fixed, without the backdoor the government would not have been able

[3] Even if the SOI returned to Remick's media without the government's knowledge despite being told not to do so, such action would still have been done by a private actor and for which the government would not be responsible.

to access Remick's media, an unacceptable option in light of the allegations of possessing CSAM and a possible sexual relationship with a minor.

- Third, the government obtained an order authorizing use of a pen register/trap and trace device on Remick's IP address on June 25, 2021. (Misc. no. 2:21-mc-100, Doc. 2). It authorized monitoring of Remick's IP address, which included monitoring done by the SOI.[4]

- Lastly, the government obtained the warrant to search Remick's media on July 2, 2021. The Alarm alerted the following day. Therefore, when the Alarm went off, the government had a warrant to access Remick's media and lawfully received that information.

The suggestion that the government continuously monitored and relied on the Alarm to plan its investigative activities is incorrect. The government moved quickly to obtain the Warrant because it had information that Remick possessed CSAM and was possibly in a sexual relationship with a minor. It obtained the Warrants on July 2, 2021 and planned to execute the Remote Access Warrant on July 6, 2021. When the SOI told the government the Alarm had alerted, on July 3, 2021, the case agent hesitated to commit to executing the Warrant that day because the government had not planned to execute then. Ultimately, of course, the government executed the Warrant that day, despite its original operational plan. In addition, once the Remote Access Warrant was issued the government had 14 days to execute it, regardless of what happened with the Alarm. The government would have executed the Warrant in that time period and accessed whatever media it could. The government did not rely on the Alarm in its operational planning.[5]

---

[4] Remick's ISP did not provide timely information in response to the pen register/trap and trace order and was not relied upon.

[5] Candidly, while the government acknowledges that the SOI disclosed the fact of an Alarm to it, its full capabilities were not understood by the government until after it alerted on July 3, 2021. If the Alarm had been fully understood, the government would have proceeded much differently, as seen above.

In that vein, it is critical to recognize exactly what the Alarm did. The Alarm did not capture files or other content from Remick's computer; its purpose and function was to alert the SOI when the VeraCrypt container was mounted. The balance of Remick's digital media was accessible to the government through its exploitation of the vulnerability discovered by the SOI. The defense request to suppress all of the evidence because of the Alarm, therefore, seeks too much. Assuming *arguendo* that the government erred in its conduct surrounding the Alarm and the Court believes a sanction is appropriate, only evidence from digital media affected by the error, the mounted VeraCrypt container, should be suppressed. The evidence found during the searches on Remick's other media, including thousands of thumbnail images of CSAM, password files, email communications, and other content, should be admissible.

This case is analogous to the private actor finding in *United States v. RW Professional Leasing Services Corp.,* 384 F. Supp. 2d 566 (E.D.N.Y. 2005). There, a contractor (Zambaras) told the FBI about fraudulent activities being done by RW Professional Leasing Services Corp. (PLS). Zambaras also told the FBI about evidence of the fraud he had taken without authority. The agent admonished Zambaras for removing the materials, and directed him to retain it. Zambaras met with the agent a second time and gave the materials to her. The agent accepted them and used them to obtain a search warrant . PLS moved to suppress the warrant. The district court distinguished *Knoll* because in *Knoll*, there was "testimony that the government agent encouraged the private party after learning of the surreptitious search by making statements such as 'get me more information[.]'" *Id.* at 571. The district court wrote:

> In this case there was absolutely no evidence that the government directed, encouraged, or tacitly approved of Zambaras' actions. Both Zambaras and [the agent] testified that she told Zambaras that he was not a government agent and was not authorized to take documents from PLS. After their first meeting, [the agent] did not encourage Zambaras to obtain additional documents. Rather, she repeatedly admonished Zambaras for taking the materials. Also, instead of asking

> Zambaras to seize additional evidence, [the agent] immediately sought advice from an Assistant United States Attorney and a search warrant from the court. In sum, there is absolutely no evidence in the record that the government directly or tacitly approved the search and seizure executed by Zambaras.

Id. at 571.

In the case at bar, when law enforcement learned of the SOI's conduct, it immediately instructed him not to reenter Remick's media. While it spoke to the SOI, its questions were targeted to learn what the SOI had observed, not to have him gather more information. The agents immediately involved the U.S. Attorney's Office. The government quickly sought and obtained a warrant to search Remick's media. Suppression is not appropriate.

B. <u>The Affidavit Demonstrated Probable Cause to Search</u>

1. Statement of the Law

The Fourth Amendment to the Constitution provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend IV. Probable cause is "'a fluid concept,' turning 'on the assessment of probabilities in particular factual contexts,' and as such is not 'readily, or even usefully, reduced to a neat set of legal rules.'" *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232 (1983)). Whether probable cause exists "'requires a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *United States v. Martin*, 426 F.3d 68, 74 (2d Cir. 2005) (quoting *Illinois v. Gates*, 462 U.S. at 238). "The inquiry turns on an 'assessment of probabilities' and inferences, not on proof of specific criminal conduct beyond a reasonable doubt or even by a preponderance of the evidence." *Id*. at 76. It is a "relaxed standard, not a legal determination of guilt or liability." *Id.* (citations omitted). When construing

an affidavit to assess probable cause, the affidavit should be taken as a whole and read realistically. *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998).

A reviewing court is to accord "substantial deference to the finding of an issuing judicial officer that probable cause exists." *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)). The reviewing court's inquiry is limited to evaluating whether the issuing judge had "a substantial basis" to determine that probable cause existed and the warrant should issue. *Id.*

2. Argument

Remick claims that the affidavit filed in support of the search warrant failed to provide a sufficient basis for believing that what the SOI saw on Remick's media was, in fact, CSAM. This claim should fail.

The affidavit contained the SOI's descriptions of three images that he recalled from memory. (Doc. 5-3 at ¶ 18). In the first image, the SOI provided an age of the child (approximately 10-14 years old) engaged in the sex act, which he colloquially described and the affiant defined as two individuals simultaneously performing oral sex on each other. (¶ 18a). As to the second image, the SOI provided an age for the child (approximately 12-13 years old), the basis for that approximation (no pubic hair or breast development observed), and a description of what the child was doing (legs spread wide open). (¶ 18b). For the third image, the SOI provided an age for the child (approximately 15-16 years old) and noted that her breasts were exposed. (¶ 18c).[6]

[6] The government agrees that the third image as described does not constitute CSAM pursuant to 18 U.S.C. § 2256. The presence of this image, even though it is child erotica and not CSAM, still bolsters the probable cause finding because its possession demonstrates Remick's sexual interest in children.

As this Court observed in *United States v. Barker,* 2012 WL 12543 (D.Vt. Jan. 3, 2012), expert testimony is not required "regarding children depicted in images of child pornography as a condition precedent to a valid search warrant." *Id.* at *6 (rejecting claim that search warrant affidavit needed to establish that real children were depicted in the images). Indeed, the Court cited approvingly to cases sanctioning the use of lay witnesses to establish that images found in a defendant's collection depicted children engaging in sexually explicit conduct:

> *See United States v. Battershell,* 457 F.3d 1048, 1054 (9th Cir. 2006) ("Indeed, we have accepted, for purposes of an affidavit in support of a search warrant, the conclusory age estimates made by civilians and other untrained lay witnesses without demanding a detailed explanation of how the witnesses reached that conclusion."); *United States v. Hall,* 142 F.3d 988, 995 (7th Cir. 1998) (accepting computer repairman's statement that images on computer showed "minors"); *United States v. Bonczek,* 2008 WL 4615853, at *11 (S.D.N.Y. Oct. 16, 2008) (concluding detective's "representations that the images were of young children, 'with genitalia exposed,' and 'posed in a sexually explicit manner' provided [the judge] with sufficient information to find that probable cause existed to believe that [defendant's] apartment and computer contained images of child pornography.").

Id. at *6. *See also United States v. Wiegand,* 812 F.2d 1239, 1243 (9th Cir. 1987) ("Common sense suggests that most of the time one can tell the difference between a child and an adult.")

In addition to the SOI's observations of what images he saw on Remick's computer, the affidavit contained other evidence that provided support for the Magistrate Judge to credit the SOI's report that he saw CSAM. The SOI provided the text file that included file titles he pulled from Remick's computer. These file titles obviously referenced CSAM and included "10Yo Girl Spreads And Plays With Hairless Pussy For Webcam - 2004.avi" and "Julia 7yo – First Assfuck.avi.avi." SA McCullagh added that he recognized phrases on the text file that "are used to identify child exploitation material." (Doc. 5-3 at ¶ 8b). SA McCullagh also saw two folders on the text file named "For Jeanie/Pearl Lolitas" and "For Jeanie/Videos." SA McCullagh knows that "the term 'Lolita' can refer to child pornography." (Doc. 5-3 at ¶ 9e). The SOI also

saw evidence that Remick used the Tor browser, which is known to SA McCullagh to be "commonly used by persons who are interested in child pornography because the user's identify is, generally, obscured." (Doc. 5-3 at ¶ 9c).

In addition, Remick's media contained extremely sophisticated levels of encryption and used a virtual private network, which indicates his intention to hide their contents. This is something that Remick, a computer expert with a self-described "unmatched skill set," could easily accomplish. (Doc. 5-3 at ¶¶ 9b, 10c, and 13).

Importantly, the affidavit included that in coming forward to let law enforcement know that Remick possessed CSAM, the SOI revealed his illegal intrusion into Remick's media and exposed himself to criminal liability. The SOI's statements against self-interest enhanced his credibility.

Law enforcement was also able to corroborate aspects of the SOI's information. The Vermont driver's license was legitimate. The IP address he provided resolved back to Remick. The sophistication of Remick's encryption and network was consistent with his status as a computer expert.

Remick claims that inclusion of descriptions of only three images when the SOI said that he saw seven means that the other four images were not CSAM. (Motion at 13-14). That is not what is written in the affidavit. Rather, at paragraph 18, SA McCullagh wrote the following about his June 23, 2021 meeting with the SOI:

> During this conversation, the SOI provided a description of several of the child pornography and child exploitation images from memory; the SOI did not save any of the image files it viewed. A description of some of the files are below.

Remick's conclusion that the other four do not constitute CSAM is not supported by the record.

Remick's skepticism about the SOI's stated reaction that it "shook me to my core" to see CSAM because the described images would not justify that reaction, is remarkably jaded. (Motion at 14). While the litigants and the Court have seen far too many CSAM images, that sad familiarity cannot result in criticism of lay persons who have never seen such images and have a strong negative reaction.

Remick's additional criticism of the SOI for not saving copies of the CSAM he saw is similarly misplaced. (Motion at 14 n.3). The SOI obviously recognized that what he saw on Remick's media was illegal, which is why he reported Remick to law enforcement in the first place. The SOI can hardly be faulted for choosing not to take possession of the contraband itself, even assuming he knew of the affirmative defense. Further, the SOI had a strong visceral negative reaction to viewing the images. It is understandable that he would not want to possess that which upset him so much. Based on the foregoing, it is clear that the Magistrate Judge had a sufficient basis to find probable cause to issue the warrant. Its finding should not be disturbed.

C. The Warrant Was Sufficiently Particular

1. Statement of the Law

The Fourth Amendment provides that a "warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). By ensuring that the search is limited to specific areas and things for which there is probable cause to search, the particularity requirement "ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). In assessing the Constitutional sufficiency of any

warrant, courts must be mindful that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006).

To satisfy the particularity requirement, a warrant must satisfy three criteria. *See United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). It must: (i) "identify the specific offense for which the police have established probable cause;" (ii) "describe the place to be searched;" and (iii) "specify the items to be seized by their relation to designated crimes." *United States v. Ulbricht*, 858 F.3d 71, 98-99 (2d Cir. 2017), overruled on other grounds by *Carpenter v. United States*, 138 S.Ct. 2206 (2018); *Galpin*, 720 F.3d at 445-46.

While "breadth and particularity are related," however, they are also "distinct concepts," and a "warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material," without necessarily "violating the particularity requirement." *Ulbricht*, 858 F.3d at 102; *see also United States v. Scully*, 108 F. Supp. 3d 59, 69 (E.D.N.Y. 2015) (generally, a warrant that authorizes a search for documents and things that constitute evidence of a particular crime is not overbroad).

2. Argument

In his claim that the Remote Access Warrant was not sufficiently particular, Remick claims only that the government should have identified and confined its search to the specific computer the SOI accessed. This claim should be dismissed.

It is fundamental that search warrants are issued based on the court's determination that probable cause exists to believe that evidence of a crime will be found at a particular location. Law enforcement is authorized to search that location in any place where the evidence could be found. In the usual case where CSAM is discovered because it was shared by a device using an IP address that resolves to a residence, law enforcement obtains a search warrant for the entire

residence. All locations where contraband might be located, including all devices present at that residence when the warrant is executed, are subject to search because it is not known which device used the IP address to share contraband. Law enforcement is not required to stop once it recovers some contraband. A drug search warrant does not stop when some drugs are found; it stops when the entire location where drugs could be found has been searched. The same holds true in execution of CSAM search warrants.

The only difference in execution of the remote access warrant versus the traditional warrant was the means of entry. Instead of entering through the front door and checking all of the media at the residence, the government entered the media remotely using the IP address. All devices accessible through the IP address were subject to search because until the contents of the media were examined, it could not be known whether they contained contraband that the issuing court found probable cause to believe would be found there. Moreover, the SOI observed that the network contained at least two computers and three VeraCrypt containers. It was entirely reasonable for the court to authorize the search of all devices accessible through the IP address based on the information in the affidavit.

Remick is thus in the ironic position of complaining that the SOI, when it infiltrated his computer, did not take enough information so the government could narrow its search. Even if the SOI had taken additional identifying information, like the Global Unique Identifer the defense suggests (Motion at 16), finding that information would necessarily have required accessing the digital media accessible through the IP address. The Warrant was sufficiently particular.

D. Execution of the Search Was Reasonable

1. Statement of the Law

There is no requirement that the manner of execution of a search warrant be included in the warrant. In *Dalia v. United States*, 441 U.S. 238 (1979), the Supreme Court held that officers executing a Title III order authorizing interception of oral communications acted reasonably when they made a surreptitious entry to install an electronic bug even though the Title III order did not authorize the covert entry. The Court held that "[n]othing in the language of the Constitution or in Court's decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed." *Id.* at 257. The Court further recognized that executing officers "may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant" and that "the details of how best to proceed with the performance of a search authorized by warrant" are "generally left to the discretion of the executing officers." *Id.*

The fact that a warrant need not specify its manner of execution, however, does not mean that the Fourth Amendment does not constrain how a warrant is executed. Instead, the "manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia*, 441 U.S. at 258. "The general touchstone of reasonableness which governs Fourth Amendment analysis, governs the method of execution of the warrant." *United States v. Ramirez,* 523 U.S. 65, 71 (1998) (internal citation omitted) (reasonableness of no-knock warrant). Moreover, although the Supreme Court in *Dalia* held that the government was not required in its affidavit to disclose its planned covert entry to install the bug, it noted that the "preferable approach" would be for the government to do so. *Dalia*, 441 U.S. at 259 n.22.

2. Argument

Remick claims that the government relied on the "SOI's untested and unverifiable hacking method" to gain access to his network. Remick's complaint is without merit.

To begin, to the extent the government used the SOI code as the foundation for its own, such use was not unreasonable because the SOI's code worked. The SOI successfully accessed Remick's media. In any event, the government did not use the SOI's code because, as previously indicated, COO Brigham modified it to create the HSI Code, which was used to conduct the exfiltration. After writing the HSI Code, COO Brigham recreated on a government computer what he understood the configurations of Remick's media to be, including the vulnerability the SOI exploited. Brigham tested the HSI Code and confirmed that it would work. It was only then that it was used to exfiltrate content through execution of the Remote Search Warrant. The government's method of executing the Warrant was reasonable, and it appropriately notified the issuing court of its intentions.

E. Remick Has Failed to Meet His Burden to Obtain a Franks Hearing

1. Statement of the Law

The Supreme Court held in *Franks v. Delaware* that search warrant affidavits are entitled to "a presumption of validity." 438 U.S. 154, 171 (1978). To overcome this presumption and obtain an evidentiary hearing on the truthfulness of a search warrant affidavit, a defendant must overcome a two-step hurdle, each supported by an offer of proof. *Id.* at 155-56, 171. A defendant must show that "(1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause . . . finding." *United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013).

To determine whether an allegation of deliberate or reckless falsity meets this standard, the Court looks to the affiant's subjective intent. The *Franks* standard "protects against omissions that are designed to mislead, or that are made in reckless disregard of whether they would mislead, the magistrate." *United States v. Awadallah*, 349 F.3d 42, 68 (2d Cir. 2003) (quoting *United States v. Colkley*, 899 F.2d 297, 301 (4th Cir. 1990)). "Allegations of negligence or innocent mistake are insufficient." *Franks*, 438 U.S. at 171.

To determine whether alleged omissions were material to the finding of probable cause, the Court "insert[s] the omitted truths" and asks "whether, after . . . correcting material omissions, there remains a residue of independent and lawful information sufficient to support a finding of probable cause." *Rajaratnam*, 719 F.3d at 146 (alterations omitted) (quoting *United States v. Ippolito*, 774 F.2d 1482, 1487 n.1 (9th Cir. 1985); *United States v. Canfield*, 212 F.3d 713, 718 (2d Cir. 2000)). If the affidavit provides probable cause with the omitted information included, no hearing is required. *Id.* at 146; *see also Franks*, 438 U.S. at 171-72.

For the required allegations to establish the need for a *Franks* hearing, they "must be more than conclusory and must be supported by more than the desire to cross-examine." *Franks*, 438 U.S. at 171. The defendant's allegations "must be accompanied by an offer of proof." *Id.* In other words, the defendant should provide the reviewing court with "[a]ffidavits or sworn or otherwise reliable statements of witnesses" or at least "satisfactorily explain[]" the absence of such proof. *Id.*

2. Argument

Remick advances four grounds upon which he claims should be explored at a *Franks* hearing. Each of the grounds is insufficient to trigger holding a hearing.

The first claim is that the affidavit should have informed "the [M]agistrate [Judge] that the remote access will be achieved through unknown, untested, and unverified methods" and had the court been so informed, it "would have declined to issue the warrant." (Motion at 20). As previously examined, *infra* at 9-10, Remick's factual assertion is incorrect as the exfiltration of Remick's media was conducted using the HSI Code, which COO Brigham developed and tested prior to its use. Moreover, the caselaw is clear that the government is not required to disclose to the issuing court how a search warrant will be executed as such matters are properly left to the discretion of law enforcement. *Dalia*, 441 U.S. at 257. That said, the government did provide the general framework of how the Remote Access Warrant would be executed because that is the preferred method. *Id.* at 259 n.22. There was no material false statement to the issuing court and there is no basis for a *Franks* hearing.

The second claim is that the government withheld information about the Alarm installed by the SOI during its intrusion. (Motion at 20-21). As previously discussed, *infra* at 10, 12-14, the government did not rely on the backdoor or Alarm, placed in Remick's media by a private actor without the government's knowledge, in its planning and was caught off-guard when the Alarm alerted. More importantly, the Alarm had nothing to do with whether there was probable cause to issue the Remote Access Warrant and, therefore, was not material. If this information had been included in the affidavit, the evidentiary foundation for the probable cause finding and issuance of the Warrant would have remained. The Alarm does not provide a basis for a *Franks* hearing.

Third, Remick claims that the government should have included information from the NCMEC report, specifically that neither Remick, his address (residence and IP), or his telephone number were the subject of prior NCMEC reports. He claims that these omissions allegedly

weigh "strongly against the SOI's claims." (Motion at 21). This claim must fail. The SOI did not claim that Remick was the subject of any prior NCMEC reports; the SOI claimed that he saw CSAM on Remick's network and provided a text file with file titles consistent with what he saw. There was no reason to include the lack of NCMEC reports because there was nothing from the SOI to rebut. Further, the absence of this information allowed the issuing court to assume, reasonably, that there were no prior reports because if there were, the government would have included them. It should be recalled that Remick used a VPN, meaning his actual IP address was hidden and would not have been the subject of a NCMEC report. That there was no mention of Remick's criminal history similarly inured to his benefit. These omissions were not material and provide no basis for a *Franks* hearing.

Remick objects to inclusion of the SOI's lack of criminal history in the affidavit and suggests that the SOI's credibility was thereby bolstered, but the failure to include that Remick also did not have criminal history was unfair. Remick misses the point. The government included information about the SOI's criminal history, as well as his agreements with the government and information about his mental health challenges, so the Magistrate Judge had the pertinent information with which to assess the SOI's credibility when deciding whether to credit the SOI's information and issue the Warrant. The foregoing does not provide the basis for a *Franks* hearing.

Lastly, Remick claims that the government inappropriately withheld information about Jean Lin, an adult, which if included would have cast doubt on the ability of the SOI to assess the age of children in the images it saw. Remick's asserts that the "SOI must have formed this opinion based on images of this individual that it found when it hacked the computers." (Motion at 22). This claim must also fail. It is unknown whether the SOI ever saw a picture of Jean Lin.

The leap Remick asks the Court to take, that since the SOI could not correctly identify Jean Lin's age, it could not be counted upon to estimate the ages of the children seen in the images it described, thus has no foundation. The government did not err in failing to include that Jean Lin is an adult.

Moreover, the SOI deduced from communications that Jeanie "may be a teenager" and that she and Remick "are either trading images or having a relationship."[7] (Doc. 5-3 at ¶ 17). SA McCullagh found a folder in the text file provided by the SOI titled "For Jeanie/Pearl Lolitas," and he knows the term "Lolita" can refer to child pornography. (Doc. 5-3 at ¶ 9(e)(1)). The foregoing gave weight to the concern that Remick might be trading CSAM images, and the age of the person with whom he was possibly trading was irrelevant. There is simply no basis for Remick's complaint that the government did not disclose that Jean Lin was an adult.

F. <u>The Agents Relied in Good Faith on the Search Warrants</u>

1. Statement of the Law

Even if this court were to conclude that the Remote Search and Hardscrabble Road Warrants were inconsistent with the Fourth Amendment, a suppression remedy would not be appropriate. The Supreme Court has rejected suppression of evidence obtained by officers acting in objectively reasonable reliance on a search warrant. *See United States v. Leon*, 468 U.S. 897, 926 (1984). More generally, Supreme Court precedent dictates that suppression is a remedy of last resort, to be used for the sole purpose of deterring future Fourth Amendment violations, and only when the deterrence benefits of suppression outweigh its heavy costs. *See Davis v. United States*, 564 U.S. 229, 237 (2011*); Herring v. United States*, 555 U.S. 135, 140-41 (2009).

[7] It should be recalled that in its initial conversations with law enforcement, the SOI thought that Remick was speaking with someone named "Jenny" or "Jennie," not Jean.

The exclusion of evidence is a "prudential" remedy created by the Supreme Court, and not a requirement for every violation of the dictates of the Fourth Amendment. *Raymonda*, 780 F.3d at 117. Because the exclusionary rule was designed to deter government misconduct, it is inapplicable when suppression would provide only marginal deterrence. *Id.* Instead, the rule applies only when police exhibit "deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights." *Id.* at 118. Therefore, for agents who obtain evidence by objectively reasonable reliance on a warrant obtained from an impartial magistrate judge and there is no conscious violation of the Fourth Amendment, and therefore nothing to deter. *Id.*

Based on *Leon*, the Second Circuit has identified only four limited circumstances where the good-faith exception to the exclusionary rule does not apply to a search warrant:

> (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.

United States v. Clark, 638 F.3d 89, 100 (2d Cir. 2011) (quoting *United States v. Moore*, 968 F.2d 216, 222 (2d Cir. 1992)).

2. Argument

None of these four circumstances is present in this case. The government did not knowingly mislead the Magistrate Judge. Indeed, the government endeavored to be as transparent with the court as possible in light of the novelty of the situation. There can be no realistic contention that the Magistrate Judge "wholly abandoned" his judicial role. There was ample probable cause to support the Warrant's issuance. The Warrants were not so facially deficient that the government's reliance on them was unreasonable. The other factors identified

by Remick in the Motion to find a lack of good faith were addressed and discounted earlier in this opposition.

Lastly, Remick claims that the government was willing "to credit and rely on the SOI's fabulous tale" recklessly and with indifference to his Fourth Amendment rights. That is simply not correct. The government collected the SOI's information, corroborated it where possible, and submitted it to the neutral magistrate for its consideration of whether to issue search warrants. That is exactly what is required by the Constitution and Rule 41. The government acted appropriately and was entitled to rely on the Warrants in good faith.

VI. CONCLUSION

For all of the foregoing reasons, the government respectfully requests the Court deny Remick's request for a *Franks* hearing, and deny the Motion in its entirety.

Dated at Burlington, Vermont, this 21st day of February, 2023.

Respectfully submitted,

NIKOLAS P. KEREST
United States Attorney

By: */s/ Barbara A. Masterson*
BARBARA A. MASTERSON
Counselor to the U.S. Attorney
P.O. Box 570
Burlington, VT 05402
(802) 951-6725